Atty. Dkt. No. 061602-6000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	PIENIMAKI et al.
Title:	FORCED ENCRYPTION FOR WIRELESS LOCAL AREA NETWORKS
Appl. No.:	10/679486
Filing Date:	10/7/2003
Examiner:	GEE, Jason Kai Yin
Art Unit:	2434
Confirmation Number:	4042

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the New **Pre-Appeal Brief Conference Pilot Program**, announced July 11, 2005, this Pre-Appeal Brief Request is being filed together with a Notice of Appeal.

REMARKS

In the outstanding Office Action of September 18, 2009, the Examiner maintained the rejection of claims 1, 2, and 5-12 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2004/0203783 (Wu et al.) Applicant traverses the rejection.

With regard to independent claims 1, 7, and 10 of the present application, the Examiner again asserted that Wu et al. teaches all of the required limitations recited therein including "enforcing an application to switch any traffic provided over internet access to the user terminal in the public wireless local are network to an encrypting security service port."

In making the above assertions, the Examiner continued to rely on paragraphs [0012], [0030], [0031], and [0039]-[0041] of Wu et al. (*See, e.g.,* page 4 of the outstanding Final Office Action). Additionally and at pages 2-3 of the outstanding Final Office Action, the Examiner further responded to the arguments presented in Applicant's July 10, 2009 Reply. To support these assertions, the Examiner cited to Figures 2 and 4, and paragraphs [0003], [0006], [0007], [0025]-[0029] of Wu et al. It appears that in the Examiner's opinion, because Wu et al. teaches that a terminal is able to access the Internet in the system of Wu et al., the encryption taught by Wu et al. (in the context of authentication during a handover) necessarily teaches and suggests that the same encryption is forced/enforced on traffic provided over Internet access. Applicant emphatically disagrees with the Examiner's position.

As previously described at length in Applicant's July 10, 2009 Reply, Wu et al. is directed to a system and method for enabling a wireless terminal to handoff between a first and second access point (AP), where various authentication procedures are performed including certain encryption processes. (See, e.g., Abstract and paragraph [0006] of Wu et al.) However, Applicant again submits that the teachings of Wu et al. "end" at the authentication process. That is, Wu et al. fails to teach or suggest performing any operations "after" the terminal is authenticated/authorized at the second AP.

Figure 2 and paragraph [0003] of Wu et al. merely teaches that terminals may communicate with a larger network (presumably the Internet) via a WLAN, where an "access point" (AP) is a terminal that "acts as a gateway between the WLAN and the larger network." Applicant submits that this is no more than a general description of WLANs and is neither suggestive nor evidence that the encryption of handoff/session WEP keys between a terminal and an AP is inherently applied to/encompassing of communications over Internet access. Moreover, paragraphs [0004]-[0005] of Wu et al. go further to describe that the reason for the invention described therein is to provide a system and method of <u>authenticating</u> a terminal with an AP in the context of handover from a first AP to a second AP.

At page 2 of the Final Office Action, the Examiner asserted "[t]hese access control points are ultimately controlled by the AAAH and AAAF servers, as seen in paragraphs 25-29." Applicant disagrees. First, Applicant notes that nowhere prior to this sentence of the outstanding Final Office Action, nor anywhere in Wu et al., is the term "access control point" ever mentioned, described, or suggested. To wit and as discussed above, Wu et al. explicitly defined AP to mean a gateway between a WLAN and larger network. Therefore, Applicant submits that Wu et al. already fails to teach or suggest any access control point.

Second, Applicant notes that Wu et al. is also explicitly clear in describing the role of the AAAH/F's. That is, AAAH/F's are merely authentication, authorization, and accounting home/foreign servers, which serve to authenticate a terminal with either a home or foreign AP "during a handover." The only other role/function of an AAAH/F beyond authentication of a terminal to an AP is, i.e., to "determine" whether a terminal may have access to a network/resource, and tracking (accounting for) such resources utilized. (*See, e.g.,* paragraphs [0025] and [0029] of Wu et al.) There is neither an explicit nor an implicit suggestion that the AAAH/F servers "control" anything beyond authentication to an AP.

Paragraphs [0006]-[0007] of Wu et al. describe transmitting a handoff WEP key from a first AP to a terminal to effectuate a handoff to a second AP. However, the Examiner improperly extrapolated such procedures, "[w]hen the access point hands off the handoff key to the user to authenticate himself with another access point, this is enforcing the terminal to switch its traffic to an encrypting security service port which is another access point."

First and to the above, independent claims 1, 7, and 10 of the present application require not merely switching "traffic" to an encrypting security service port, but switching "any traffic <u>provided over internet access to the user terminal</u> in the public [WLAN] to an encrypting security service port." That is, the Examiner appears to have improperly construed the recited limitations of the present application by not taking into account the type of traffic claimed. Even if the Examiner's intent was to encompass such Internet traffic, Applicant still submits that in no way can the transmission of a handoff key "from" an access point" to effectuate a handover be reasonably interpreted to read on Internet traffic. Moreover and contrary to the Examiner's unsupported "extrapolation," Wu et al. is explicitly clear in describing the encryption described therein is applicable to "terminal authentication packets," nothing more. (*See, e.g.,* [0008], [0027], [0037] of Wu et al.) Further still, Wu et al. even admits that "[a]gain, however, encryption of the terminal authentication packets may <u>not</u> be necessary." (emphasis added). (*See, e.g.,* paragraph [0057] of Wu et al.) Applicant submits that Wu et al. cannot be interpreted to read on independent claims 1, 7, and 10 of the present application, which requires "enforcing an application to switch…to an encrypting security service port" when Wu et al. does not necessarily encrypt the terminal authentication packets that the Examiner has asserted must be encrypted.

Second and to the above, Applicant submits that contrary to the Examiner's assertions, nothing in Wu et al. is even remotely suggestive of an "encrypting security service port" as required in independent claims 1, 7, and 10 of the present application. As noted above, the Examiner has asserted that such an encrypting security service port is analogous to an AP of Wu et al. Applicant again emphatically disagrees. Paragraph [0012] of Wu et al. explicitly describes an AP to have a memory that includes instructions to "receive" a packet and "delete" the packet if not encrypted (already) with a handoff WEP key, as well as decrypting and transmitting the packet that is (already) encrypted. Paragraph [0037] of Wu et al. further describes that APs "may only allow the terminal to communication terminal authentication packets with an authentication server. After the terminal has been authenticated… the access points may allow the terminal to communicate date packets via the network." Moreover, Applicant directs that Examiner to, e.g., page 5, lines 21-25 of the present application, which describes that the access control point "forces applications X to switch the traffic to an encrypted port" such as according to SSL or TLS. Examples of such traffic, TCP/IP traffic, HTTP traffic, mail, etc. are described at page 6, lines 1-9 of the present application as well (none of which may be analogized to, e.g., terminal authentication packets such as those described in Wu et al.) That is, Wu et al. is abundantly clear in that an AP at best may "decrypt" terminal authentication packets, but in no way does an AP read on a security service port that "encrypts" traffic over internet access as required in the present application claims. Moreover, Wu et al. is again clear in that only after a terminal is authenticated (via, e.g., the handover/session WEP key) may it communicate with the network (which as described in paragraph [0003] and interpreted by the Examiner to be, e.g., the Internet), where Wu et al. makes no suggestion that such communication (application) is necessarily enforced to switch such communication traffic over internet access to an encrypting security service port.

With regard to the Examiner's reliance upon Figure 4 of Wu et al. as alleged evidence that AAAH/F servers enforce some encryption policy (directed to handover), and thus the terminal would not be able to connect to other APs, Applicant again directs the Examiner to, e.g., paragraph [0057] of Wu et al., which is part of the corresponding description of Figure 4. Again, paragraph [0057] of Wu et al. indicates that it is not even necessary to encrypt the terminal authentication packets of Wu et al. Moreover and again, Figure 4, offers no support for the Examiner's assertions as it merely describes an "open" authentication embodiment of the handover already described in Wu et al.

In contrast to Wu et al., independent claims 1, 7, and 10 of the present application at least require that an application is enforced to switch any traffic provided over internet access to the UT (in the public WLAN) to an encrypting security service port. That is, after an ACP initiates the AAA procedure for a UT and after the UT is authenticated at the AAA back-end system, the ACP forces applications to switch traffic to an encrypting security service port when the UT tries to access the Internet IP (i.e., any traffic provided over internet access).

In light of the above, Applicant submits that Wu et al. fails to teach or suggest each and every limitation recited in independent claims 1, 7, and 10 of the present application. Furthermore, because dependent claims 2, 5, 6, 8, 9, 11, and 12 are each directly or indirectly dependent upon independent claims 1, 7, and 10, Applicant submits that each of these claims are also allowable for at least the same reasons as discussed above

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance.

Respectfully submitted,

Date: January 19, 2010

By /G. Peter Albert, Jr./

FOLEY & LARDNER LLP
Customer Number: 30542
Telephone: (858) 847-6735
Facsimile: (858) 792-6773

G. Peter Albert Jr.
Attorney for Applicant
Registration No. 37,268

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) 061602-6000	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] On January 19, 2010 Signature Typed or printed name	Application Number 10/679486	Filed 10/7/2003
	First Named Inventor Sami Pienimaki	
	Art Unit 2434	Examiner GEE, Jason Kai Yin

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 37,268

□ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34

/G. Peter Albert, Jr./
Signature

G. Peter Albert Jr.
Typed or Printed Name

(858) 847-6735
Telephone Number

January 19, 2010
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.